What is claimed is:

1. A method for distributively managing the certificate revocation list (CRL) in a certifying system to certify the validity of a subscriber in an open communications network such as Internet, comprising the steps of:

a) registering the certificate policy statement for the CRL by determining the distribution interval of the CRL;

b) setting the structure of the certificate of the subscriber to issue the certificate according to the registered certificate policy statement;

c) attesting the certificate by applying the distribution point mechanism according to the distribution interval to the CRL; and

d) revoking the certificate by using the distribution points to revise the CRL displayed.

2. A method as defined in Claim 1, wherein the step a) includes the steps of:

a1) defining the number N of the nodes in the directory information tree (DIT) and the hash function H() to manage the CRL based on the number of the expected subscribers;

a2) defining the subject name (SUBJECT_NAME) of the essential items constituting the certificate as the input value of the hash function;

a3) calculating the distribution interval of the CRL by using the hash function and variables; and

a4) setting the value of the variable (crl_dp_flag) for the CRL according to the distribution interval.

3. A method as defined in Claim 1, wherein the step b) includes the steps of:

b1) retrieving the subject name (SUBJECT_NAME) of the subscriber as the input of the hash function or skipping according as the certificate policy statement sets the distribution point to be applied to the CRL (crl_dp_flag=yes) or not;

b2) calculating the hash value (Vtmp) for the retrieved subject name;

b3) obtaining the interval value (n) including the hash value to complete the distinguished name (DN) of the CRL upon revoking the corresponding certificate; and

b4) issuing the certificate of the subscriber by setting the structure of the certificate by using the DN information of the CRL and the DN information of the certifying agency issuing the CRL.

4. A method as defined in claim 1, wherein the step c) includes the steps of:

c1) preparing a phrase concerning the certificate of the subscriber according to the subject name (SUBJECT_NAME) of the subscriber;

c2) requesting the certificate of the subscriber from the directory server by using the phrase to retrieve the

information of the corresponding structure from the certificate downloaded according to the subject name (SUBJECT_NAME);

c3) requesting the CRL designated the corresponding DN from the directory server according to the retrieved information;

c4) retrieving the serial number of the subscriber by checking the duration of the effective time based on the CRL; and

c5) invalidating or validating the subscriber's certificate according as the serial number is included in the CRL or not.

5. A method as defined in Claim 4, wherein the step d) includes the steps of:

d1) revising the subscriber's certificate requested for revocation in the database (DB) or skipping according as the certificate policy statement applied to the subscriber sets the distribution point to be applied to the CRL (crl_dp_flag=yes) or not;

d2) revising the CRL retrieved according to the information of the structure of the revised subscriber's certificate through the corresponding database;

d3) retrieving the reason of revoking the certificate from the packet received from the subscriber by detecting the serial number of the revised subscriber's certificate; and

d4) writing the CRL revised to include the serial number

of the subscriber's certificate and the code representing the reason of revocation into the node of the DIT managed by the directory server.

6. A computer readable recording medium storing instructions for performing a method for distributively managing the CRL in a certifying system to certify the validity of a subscriber in an open communications network such as Internet, the method comprising the steps of:

a) registering the certificate policy statement for the CRL by determining the distribution interval of the CRL;

b) setting the structure of the certificate of the subscriber to issue the certificate according to the registered certificate policy statement;

c) attesting the certificate by applying the distribution point mechanism according to the distribution interval to the CRL; and

d) revoking the certificate by using the distribution points to revise the CRL displayed.